QD-SS-001
REVISION E
EFFECTIVE DATE: December 17, 2004

ORGANIZATIONAL INSTRUCTION

PROCEDURES FOR REVIEWING HAZARD ANALYSIS

OPR(s)	**OPR DESIGNEE**
QD10, QD20, QD30, and QD40	**Sherry Jennings**

CHECK THE MASTER LIST AT: http://inside.msfc.nasa.gov/MIDL/
VERIFY THAT THIS IS THE CORRECT VERSION BEFORE USE

DOCUMENT HISTORY LOG

Status (Baseline/ Revision/ Canceled)	Document Revision	Effective Date	Description
Baseline		11/20/97	
Revision	A	6/9/99	Changes made to reflect new organization code changes and/or Changes made to reflect new directives renumbering scheme and to incorporate the corrective action for closure of NCR 266
Revision	B	11/29/99	Minor format and applicable/reference document changes.
Revision	C	9/09/02	Format and numbering change to implement requirements of QS-A-001 rev F.
Revision	D	9/24/04	Revised to bring document in compliance with the HQ Rules Review Action (CAITS: 04-DA01-0387). Changes were also made to reflect S&MA organizational name changes (i.e., QS to QD).
Revision	E	12/17/04	Administrative change – corrected numbering for proper format.

PROCEDURES FOR REVIEWING HAZARD ANALYSIS

1. PURPOSE

This work instruction defines the technical process implemented by MSFC System Safety personnel when reviewing a hazard analysis.

1.2 SCOPE

The process and procedures documented herein apply to MSFC S&MA engineers who review hazard analyses for MSFC projects including Space Shuttle, Payloads, Space Station, and Reusable Launch Vehicles (RLV).

2. DOCUMENTS

2A. APPLICABLE DOCUMENTS

2A.1 Space Shuttle Only

NSTS 22254 Methodology for Conduct of Space Shuttle Program Hazard Analyses

2A.2 Payloads Only

NSTS 1700.7 Safety Policy and Requirements for Payloads Using the Space Transportation System

NSTS 1700.7 Safety Policy and Requirements for Payloads Using the (ISS Addendum 1) International Space Station

KHB 1700.7 Space Shuttle Payload Ground Safety Handbook

NSTS 13830 Implementation Procedure for NSTS Payloads System Safety Requirements

AFSPCMAN 91-710 Air Force Requirements for Launching on an ELV

2A.3 Space Station Only

SSP 30599 Safety Review Process for the International Space Station

SSP 30309 Safety Analysis and Risk Assessment Requirements

SSP 50021 Safety Policy and Requirements

2B. REFERENCE DOCUMENTS

2B.1 All Projects

NPR 8715.3, NASA Safety Manuel

MWI 1700.2 D, System Safety Program

QD-A-005, Professional Development Roadmap for System Safety Engineers

3. DEFINITIONS

3.1 Accepted Risk - A hazard whose risk is not completely mitigated and that has been accepted by top program and safety management.

3.2 Assessment - Review or audit process, using predetermined methods, that evaluates hardware, software, procedures, technical and programmatic documents, and the adequacy of their implementation.

3.3 Catastrophic - A hazard that could result in a mishap causing fatal injury to personnel, and /or loss of one or more major elements of the flight vehicle or ground facility.

3.4 Controlled (Risk) Hazard - The likelihood of occurrence or severity of the associated undesirable event has been reduced to an acceptable level through the imposition of appropriate, readily implementable, verifiable controls which results in minimal residual risk.

3.5 Credible Condition (Event) - Condition (event) that reasonably may be anticipated and planned for on the basis of experience with or analysis of a system.

3.6 Critical - A hazard that could result in a mishap causing a nondisabling injury to personnel and/or damage to one or more major elements of the flight vehicle or ground facility.

3.7 Eliminated Hazard - A hazard that has been eliminated by completely removing the hazard causal factors.

3.8 Event Tree Analysis - An analysis that traces the effect of a mishap and leads to all possible consequences through visualization of the positive and negative aspects of each event using a type of logic tree. Event trees are complements to fault trees. This is an inductive logic method for identifying the various possible outcomes of a given initiating event.

3.9 Failure/Fault - Inability of a system, subsystem, component, or part to perform its required function within specified limits.

3.10 Fault Hazard Analysis - Analysis performed during design resulting in the identification, evaluation, and control of hazards resulting from piece-part or component faults.

3.11 Failure Tolerance - Built-in capability of a system to operate in the presence of specified hardware or software failures without the occurrence of a hazard.

3.12 Fault Tree Analysis - An analytical technique whereby an undesired state of the system is specified and the system is then analyzed in the context of its design, environment, and operation to find all credible ways in which the undesired event can occur. The fault tree itself is a graphical model of the various parallel and sequential combinations of faults that will result in the occurrence of the predefined undesired event.

3.13 Hazard - Existing or potential condition that can result in or contribute to a mishap.

3.14 Hazard Analysis - Identification and evaluation of existing and potential hazards and the recommended mitigation for the hazard sources found.

3.15 Hazard Control - Means of reducing the risk of exposure to a hazard.

3.16 Integrated Hazard Analysis - Comprehensive evaluation of hazards, taking into account all subsystems/elements which are included in the overall system being analyzed, including the system's operational and environmental envelopes.

3.17 Interface Hazard Analysis - Evaluation of hazards which cross the interfaces between a specified set of components, elements, or subsystems.

3.18 Noncompliance Report - A formal report documenting a condition in which a requirement cannot be met and the rationale for concluding that the noncompliance condition is safe.

3.19 Operating and Support Hazard Analysis - An analysis performed to identify hazards and recommended risk reduction alternatives in procedurally controlled activities during all phases of intended use.

3.20 Operating Hazard Analysis - An analysis that examines the operator interface during system operation and maintenance activities. The analysis will define certification and training requirements as well as safety inputs to technical manuals, warning signs, and safety placards.

3.21 Preliminary Hazard Analysis - A gross study of the initial system concepts used to identify all the sources that constitute inherent hazards. The sources are examined for possible

failures in every mode of system operation and methods for protecting against potential mishaps are identified.

3.22 Risk - Exposure to the chance of injury or loss. Risk is a function of the possible frequency of occurrence of an undesired event, the potential severity of the resulting consequences, and the uncertainties associated with the frequency and severity.

3.23 Risk Management - Process of balancing risk with cost, schedule, and other programmatic considerations.

3.24 Safety Analysis - Generic term associated with a family of analyses used to identify and control hazards.

3.25 System Safety - Application of engineering and management principles, criteria, and techniques to optimize safety and reduce risks with the constraints of operational effectiveness, time, and cost throughout all phases of the system life cycle.

3.26 System Safety Program Plan (SSPP) - A document that describes the safety assurance tasks to be implemented throughout a program/project or contract, including methods of approach, safety milestones, and assigned responsibilities for fulfilling these tasks.

4. INSTRUCTIONS

The approach to reviewing a hazard analysis is a 5 step process. The instructions below detail the steps to be followed in the review process. The flow diagram given in Section 12 depicts this process graphically.

4.1 Gather Data. The system safety engineer shall identify information and data resources pertinent to the system design, configuration, and operation. This activity includes identifying cognizant personnel from which data/information may be obtained, as well as collecting the actual documentation which details the design, configuration, and operations data. Pertinent information may be contained in design definition documents, performance specifications, flight and ground operations documents, conceptual and/or engineering drawings, schematics, presentation materials, and other programmatic documentation. The system safety engineer shall participate in Technical Interchange Meetings, progress reviews, requirements reviews, design reviews and other major program meetings and reviews. These meeting are typically a key source of significant information. A list of key technical discipline personnel for the project should be maintained. Questions concerning the system under study or with the documentation being collected should be directed to these personnel. Other potential sources of useful data can be obtained from previous analyses, tests, or inspections of the same or similar systems as well as from lessons learned or historical databases.

4.2 Learn the System. Before the hazard analysis can be reviewed, the system design and operation shall be fully understood by the system safety engineer. Read and study the data gathered in 5.1. Ask questions of the key technical personnel as appropriate to aid in understanding the system. In addition to an understanding of the system design and operation, the system safety policies and requirements for that system shall be thoroughly understood by the system safety engineer (e.g., NSTS 1700.7, NSTS 22254, SSP 50021, etc).

4.3 Determine the Scope and Type of Analysis that was Performed. This step will vary depending on the system that was analyzed and the life cycle phase of the project. The applicable safety requirements may be mandated by the tailored System Safety Program Plan (SSPP) or in other NASA policy and requirements documents. However, fundamental decisions in defining the scope and type of analysis that was performed which are common to all projects include: (1) deciding what was analyzed, (2) determine the level of detail of the analysis that was performed, and (3) ensuring the analysis task was focused at a manageable level. Unique project requirements are levied as follows:

a. Space Shuttle - Space Shuttle hazard analysis requirements are detailed in NSTS 22254.

b. Payloads - There are numerous requirements documents for payload hazard analysis depending on the launch/landing vehicle and the vehicle on which payload operations will occur. The following matrix provides a summary of the payload safety requirements documents.

Launch Vehicle/ Operation	Space Shuttle	ISS	Mir	ELV
Space Shuttle	NSTS 1700.7 KHB 1700.7 NSTS 13830	NSTS 1700.7 NSTS 1700.7, (Addendum 1) KHB 1700.7 NSTS 13830	NSTS 1700.7 KHB 1700.7 NSTS 13830	N/A
ELV	N/A	N/A	N/A	EWR 127-1

NSTS 13830 and EWR 127-1 define the scope and detail required in the analysis. The other documents establish safety policies and technical requirements.

c. Space Station - The hazard analysis scope and detail required for Space Station is defined in SSP 30599 and SSP 30309. The safety policy and technical requirements are defined in SSP 50021.

d. Reusable Launch Vehicle - The current requirements for RLVs are defined in the project SSPP. MIL-STD-882 provides general information regarding the scope of hazard analyses.

4.4 Perform the Review. This is not the documenting step, however, copious notes taken during this step will aid in the documentation process to follow. The system safety engineer

shall ensure the analysis is accurate with other system documentation and in accordance with the program requirements and safety documentation.

4.5 Document the Review Results. After the review is complete, the results of the review shall be documented according to the specific project requirements. Comments against a document should reference section and paragraph that is in question or does not meet program requirements.

5. NOTES

None.

6. SAFETY PRECAUTIONS AND WARNING NOTES

None.

7. APPENDICES, DATA, REPORTS, AND FORMS

None.

8. RECORDS

None.

9. TOOLS, EQUIPMENT, AND MATERIALS

None.

10. PERSONNEL TRAINING AND CERTIFICATION

Personnel involved in hazard analysis activities shall have an engineering or other approved technical background. Training in hazard analysis techniques is not required but is strongly encouraged. Training can be obtained through various courses offered periodically by the MSFC Training Branch. The training program used for System Safety Engineers at MSFC is documented in the Professional Development Roadmap (PDRM) for System Safety Engineers, document number QD-A-005.

11. FLOW DIAGRAM